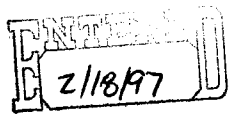
#28

February 10, 1997



Nancy Crowe
Regulatory Policy Division, Rm. 2705
Bureau of Export Administration
Department of Commerce
14th Street & Pennsylvania Ave. N.W.
Washington, D.C. 20230

Software Publishers Association

Re: SPA Comments on the Commerce Department Regulations on the Export of Encryption

Dear Ms. Crowe:

This letter constitutes the comments of the Software Publishers Association (SPA) on the new regulations on the export of encryption published in the Federal Register on December 30, 1996. 61 Fed. Reg. 68572.

The SPA is the principal trade association for the computer software industry, representing more than 85 percent of the U.S. packaged software market. Its 1200 members are both large and small software publishers and developers in the business, consumer, education, Internet and client/server markets worldwide. SPA and our members are dedicated to serving the needs of the software publishing community by addressing relevant issues and providing solutions to specific industry concerns.

Part I of our comments sets out our general thoughts and overall opposition to export controls. Part II of our comments addresses specific provisions of the regulations.

Part I - General Comments and SPA's Overall Concerns

SPA opposes export controls on encryption software. The administration's insistence on promoting key recovery and maintaining restrictions on the export of strong cryptography only serves to keep U.S. businesses at a competitive disadvantage in this growing market.

The new encryption regulations focus on promoting key recovery. However, free exportability of key recovery products is only of limited value

1730 M Street • Suite 700 • Washington, DC • 20036-4510 • Telephone (202) 452-1600 • Fax (202) 223-8756

to the software industry. SPA strongly believes that users and businesses should be able to choose the type and level of encryption appropriate to their unique situation. For some users, key recovery may be a useful feature; for others it may be completely unnecessary and undesirable. However, by forcing industry to develop such products, development costs are inflated and consumer prices rise. It is not at all clear that customer demand will justify the expense. The administration's efforts to encourage key escrow ignore the substantial market demand for unescrowed products which will inevitably be met by foreign competitors.

Moreover, even accepting the regulations' emphasis on encouraging key recovery technology, the extensive procedures that must be followed to be eligible for license exceptions for key recovery products and/or 56-bit DES products are unnecessarily burdensome and inflexible. The effect of these regulations will be to shut out small companies from a large and growing share of the software market. This portion of the software market includes any product that involves communications, networking and/or electronic commerce and financial transactions. It is these areas of the software industry that are currently experiencing dramatic growth, and where a great deal of exciting innovation is occurring. The source of much of this innovation is found in the small companies that will be most affected by these burdensome regulations.

The onerous requirements and the inability to freely export non key recovery products will put both large and small companies at a competitive disadvantage compared to foreign companies producing encryption products. There are and will continue to be many foreign software publishers that are able to fill the demand for non key recovery products. In its December 1995 study, SPA demonstrated that there were then 497 foreign products containing strong encryption available in at least 67 countries. As these foreign products increase in number and improve in quality, as they have over the last year, U.S. companies will forever lose a foothold in this growing market. What this means for American companies is lower revenues, lost market share, higher production costs and fewer jobs.

A recent example of such a foreign product is Stronghold, a commercial version of the popular Apache web server, which is available for download from the U.K. This product uses full strength, 128-bit encryption and is compatible with all major web browsers. The same company is also offering another product that is an add-on to international versions of U.S. web browsers that allows them to operate with full strength, 128-bit encryption. If such products are readily available for international distribution from one of our closest allies, there appears to be little hope of curtailing foreign availability of strong, high quality encryption products.

Thus, the new regulations force U.S. software companies to incorporate into their products a feature for which there is little or no demand, to comply

with a number of burdensome and costly regulatory requirements in order to export these products and to compete against foreign companies that are free to meet the actual demands of the market. Moreover, incorporating key recovery features is expensive and increases the cost of the product, creating another competitive disadvantage for U.S. products. The regulations also force software companies to continue the expensive practice of producing two versions of their software -- one for the domestic market (where companies are allowed to meet the demand for unescrowed encryption) and one for the foreign market (where they are not). Rather than helping to grow the market, as is the administration's claim, these regulations actually curtail any meaningful growth, virtually ceding the market to foreign competitors. This is a severe handicap for U.S. businesses seeking to enter the fast-paced, "winner-take-all" world of digital commerce.

Finally, even where there is a consumer demand for key recovery products, foreign companies will be able to offer products free of the regulatory burdens that U.S. companies must face in order to market competing products. Placing such burdens on companies wishing to market key recovery products makes their products more costly and less competitive. This result will not further the purported goal of the regulations of encouraging the development and sale of key recovery technology.

Part II - Specific Provisions of the Regulations

A. KMI License Exception Eligibility and Key Recover Agent Criteria

The eligibility requirements for license exception KMI, especially those concerning the criteria for key recovery agents, are far too burdensome to be of any practical use to the software industry.

License Exceptions

In order to qualify for the KMI license exception, the exporter of key recovery products must identify one or more key recovery agents that meet the criteria of Supplement 5 to Part 742 of the new regulations. Supplement 5 requires that agents implement a number of specific procedures designed to protect the security and confidentiality of keys. The criteria also require that the agent provide to BXA detailed information on every individual that is directly involved in the escrow of keys or other material. This information includes the individual's name, date and place of birth, and social security number (presumably not required for foreigners), as well as information indicating that he or she has no criminal convictions or pending criminal charges of any kind, has not breached any fiduciary duties and has favorable results of a credit check. The agent must also submit evidence of corporate viability and financial responsibility and must disclose any debarments, convictions or adverse civil fraud judgments. Additionally, the agent must notify BXA of any change in personnel, ownership or control.

Foreign escrow agents may be allowed if acceptable to BXA, but the requirements imposed on agents appear likely to make the approval process for foreign agents quite difficult. Similarly, the regulations allow for self escrow in certain circumstances. A key recovery agent may be internal to a user's organization, but such agents will only be approved if BXA is satisfied that the agent will respond to government requests independent of the organization and that there are adequate safeguards to ensure security and confidentiality. The regulations are unclear, however, as to whether all the normal criteria for key recovery agents apply to self escrowing organizations.

It is unlikely that foreign customers, especially those that intend to self escrow, will accept these burdensome and intrusive requirements. This is particularly true given that there are competing foreign products that do not come with these additional regulatory requirements.

Compliance Monitoring

Another aspect of these requirements could cause even greater problems for U.S. software companies wishing to sell key recovery products abroad. Section 740.8(d)(i)(E) states:

> the key recovery agent's continuing compliance with key recovery agent requirements and key safeguard procedures is a condition for the use of License Exception KMI. The exporter or reexporter, whether that person is the key recovery agent or not, must submit a new classification request to BXA if there are any changes (e.g. termination, replacement, additions) to the previously approved key recovery agent.

This language appears to require that exporters of key recovery products continue to monitor the compliance of every key recovery agent and self escrowing customer. For software companies, this requirement is simply unrealistic. Large companies sell their products to many thousands of customers, many of which will undoubtedly choose to self escrow. Tracking the continuing compliance of so many customers is simply not possible. Similarly, small software companies do not have the resources to monitor even a few customers. Moreover, customers will not buy products that require them to submit to intrusive and continual monitoring.

Exporters of key recovery software should not have an obligation to continually monitor key recovery agents and self escrowing customers. Exporters should be allowed to rely on an initial commitment by the agent or the customer to comply with BXA requirements and to notify BXA of any changes. To the extent that BXA determines that subsequent monitoring is necessary, that burden should be on BXA, not on software companies that are struggling to compete in an increasingly competitive international market.

B. Mass Market Software and the 40-bit Limit

Under the regulations, certain mass market encryption software can be released from EI controls and thereby be eligible for the same treatment as other software products and mass market encryption software that had previously been transferred to the Commerce Department through the State Department's commodity jurisdiction (CJ) procedure. The "classification request" procedure fairly closely mirrors the procedure that was available at the State Department for expedited review of CJ requests for mass market software. These requests will be processed in either seven or fifteen working days, depending upon the algorithm(s) involved.

SPA strongly believes that it is a mistake to keep the key length limit for mass market treatment at 40 bits. Instead, it should be increased to at least 56-bits. As explained below, the two-year liberalization of 56-bit products, as currently written, is of little value to the software industry. Additionally, 56-bit encryption is increasingly viewed as the minimum key length necessary to provide adequate security. Customers simply will not buy products that are limited to 40 bits, especially when there are stronger foreign products available.

C. 56-bit DES Exports and Key Recovery Plans

In order to qualify for the license exception for 56-bit non-key recovery encryption during the two-year transition period, a company must submit, and have approved, a key recovery plan. The plan must include a commitment to develop, produce and/or market key recovery products and services, and should explain in detail the steps that will be taken during the two-year transition to develop, produce and/or market encryption items and services with recoverable features. Six-month renewals of the eligibility for the license exception will depend upon adherence to benchmarks contained in the plan, and all eligibility to export these products under this provision will expire at the end of the two-year transition period.

The requirements of these plans are clearly burdensome and excessive. Most small software companies, for example, have neither the capital nor expertise to develop or incorporate key-recovery, much less have the resources to prepare a detailed plan explaining what they will do for the next two years. Software companies, especially small ones, require flexibility to change business plans on very short notice in order to respond to changes in the market. The requirements of these regulations eliminate this flexibility. As the regulations are currently written, these companies will be, in effect, completely shut out of the two-year window for DES exports.

Perhaps more important, this two-year liberalization will have no practical benefit for U.S. software companies unless, after the two-year window, those companies are allowed to continue servicing their customers who purchased the 56-bit products within the window. Similarly, customers will not buy 56-bit software products unless future versions of the software are compatible with a current version that may not incorporate key-recovery or key-escrow.

Finally, those foreign countries that maintain export controls on encryption will interpret the U.S. regulations as promoting mass exportation of 56-bit encryption. In response, these countries will likely make their 56-bit encryption products freely exportable. The difference, however, is that they will liberalize export control without the cost and regulatory burdens associated with U.S. policy. Canada, our neighbor and one of our closest allies, has done just that. The result is greater foreign competition for U.S. companies and additional costs imposed on American businesses, making their products less competitive in the global marketplace.

D. Internet Distribution of Encryption Software

Similar to State Department practice, the new regulations regard encryption software made available on the Internet, without certain safeguards, as an export. However, unlike the State Department regulations, the Commerce regulations contain unrealistic guidelines concerning these safeguards.

The guidelines included in the regulations require an access control system (either automated or human-run) that "checks the address of every system requesting or receiving a transfer and verifies that such systems are located within the United States." The system must also provide a notice that the software is export controlled, and the party seeking to receive the software must acknowledge that he or she understands that it is export controlled.

Alternatively, precautions differing from those set out in the regulations, but which are nevertheless adequate to "prevent transfer of such software outside the U.S. without a license," can be approved by BXA.

Read literally, the language used in these provisions could prevent virtually all Internet transfers of controlled encryption software. Checking a domain name or address of the systems alone cannot necessarily "verify" the location of the user. Even asking for and checking a mailing address and phone number cannot "verify" where the download is actually taking place. Similarly, no safeguards are adequate to absolutely "prevent" unlicensed transfers.

As a practical matter, reasonable steps should be designed to discourage unauthorized transfers of software outside the U.S. At a minimum, safeguards formally approved by the State Department prior to the jurisdiction transfer

should be considered adequate for the purposes of these regulations. These State Department approvals of specific procedures, and any subsequent Commerce Department approvals, should be made available to other companies seeking to distribute encryption software over the Internet.

E. Lack of Favorable End-Use and End-User Provisions

Another aspect of the new regulations that is troubling to the software industry is the lack of any provisions concerning preferential treatment for exports of non-key recovery products to certain preferred end-uses or end-users.

Under State Department jurisdiction, the government demonstrated a willingness to allow the export of encryption products that would normally be controlled (e.g. non-recovery 56-bit DES or stronger) to certain end users and/or for certain end-uses. For example, overseas banks and financial institutions have been allowed to receive such items provided their use is limited to protecting the security of financial transactions, such as in bank-to-bank communications of financial data and home banking applications. Similarly, U.S. companies have been allowed to export strong encryption products to their foreign subsidiaries in order to protect their internal corporate communications.

The Vice President's statement of October 1, 1996, stated that exports for certain financial uses would continue to receive special treatment. These regulations, however, fail to contain any codification of this practice. Many small and large software companies are developing products that will facilitate the growth of electronic commerce and other financial uses of the Internet. There is little need to incorporate key recovery into such limited products (either from a commercial or a law enforcement standpoint), and many companies rely on their ability to sell these products in the global marketplace as their primary competitive advantage. Denying the preferential treatment of non-key recovery products to these end-users will not only substantially cripple the growth of on-line commerce for the banking industry, but for all U.S. industries.

* * *

SPA strongly believes that export controls on encryption software are a tremendous obstacle for U.S. companies who want to compete globally in this lucrative market. The new regulations put forth by the administration only restrict and prohibit the growth of this vibrant and thriving sector of the U.S. economy. While the administration has voiced its support for global commerce and proposed initiatives to bring the benefits of the Information Age to schools, individuals and businesses, it has done little to bring export relief for manufacturers of encryption software. The SPA strongly encourages the

administration to reconsider the proposed regulations and lift export controls on cryptographic software products.

The SPA appreciates the opportunity to work with the administration on this important issue. Please feel free to contact either me or Lauren Hall at (202) 452-1600 if you have any questions or need any additional information.

Sincerely,

Ken Wasch

Kenneth Wasch
President
Software Publishers Association